

👤 ประชาสัมพันธ์

🌟🌐 รู้ทันกลโกงออนไลน์ ป้องกันตัวเองก่อนตกเป็นเหยื่อ 🚨

องค์การบริหารส่วนตำบลบางตาเถร ขอประชาสัมพันธ์ให้ประชาชนรู้ทันรูปแบบการหลอกลวงทางออนไลน์ (Scammer) ผ่านอินโฟกราฟิกความรู้ จำนวน 4 เรื่อง

1. สด. เตือน ระวังเพจปลอม อบจ. เทศบาล อบต. และหน่วยงานของรัฐ
2. เด็กก็เสี่ยง อย่าหลงเชื่อ เปิดบัญชีม้า
3. รู้ทันกลโกง หลุมดอชญากรรมไซเบอร์ คาถาป้องกันภัย “ไม่เชื่อ ไม่รับ ไม่โอน”
4. ระวัง รักออนไลน์ อาจเป็นกับดักหลอกโอนเงิน

🚨 ก่อนเชื่อ ก่อนคลิก ก่อนโอนเงิน ตรวจสอบข้อมูลให้รอบคอบ

💡 จำให้ขึ้นใจ “ไม่เชื่อ – ไม่รับ – ไม่โอน”

สด. เตือน! ระวัง! เพจปลอม
อบจ. เทศบาล อบต. และหน่วยงานของรัฐ

ลักษณะเพจปลอม

1. ชื่อเพจ **ระกณิด** หรือใช้โลโก้คล้ายของจริง
2. **เพียงสร้างเพจ** ผู้ติดตามน้อย
3. โพสต์แจกเงิน ทุ้เงิน ลงทุน หรือรับสิทธิพิเศษ
4. ส่งลิงก์ หรือ QR Code ให้กด
5. ขอ เลขบัตรประชาชน เลขบัญชี หรือ OTP

วิธีป้องกัน

1. ตรวจสอบชื่อเพจและเครื่องหมายยืนยัน
2. เข้าเว็บไซต์หรือเพจทางการของหน่วยงานโดยตรง
3. ไม่กดลิงก์จากข้อความแปลก
4. ไม่เปิดเผยข้อมูลส่วนบุคคลและ OTP
5. โทรสอบถามหน่วยงานก่อนเชื่อ

จำไว้! หน่วยงานของรัฐ **ไม่มีนโยบาย** ให้โอนเงินเพื่อรับสิทธิ และ **ไม่ขอรหัส OTP**

ไม่เชื่อ ไม่รับ ไม่โอน

กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ด้วยความปรารถนาดีจาก กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

รู้ทัน กลโกง หลุมดอชญากรรมไซเบอร์
คาถาป้องกันภัย “ไม่เชื่อ - ไม่รับ - ไม่โอน”
3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์

1 กลโกงยอดฮิตที่ต้องระวัง

- ▶ ปลอมเป็นเจ้าหน้าที่รัฐ เทศบาล / อบต.
- ▶ อ้างเป็นหน่วยงานหลัก
- ▶ ขอใช้คดลิงก์
- ▶ ขอโอนเงิน
- ▶ เพจปลอม / เว็บไซต์ปลอม
- ▶ แฉกของรางวัล
- ▶ รับสิทธิพิเศษ
- ▶ หลอกล่อข้อมูล
- ▶ SMS / ลิงก์ปลอม
- ▶ ส่งลิงก์ที่แปลก
- ▶ หลอกล่อให้ตอบ
- ▶ กดข้อมูล
- ▶ ขอเลขบัตรประชาชน
- ▶ ขอเลขบัญชี
- ▶ ขอ OTP
- ▶ หลอกลวงออนไลน์
- ▶ หลอกลวงลงทุน
- ▶ ทำเร็ว
- ▶ ไม่มีความเสี่ยง

2 จำให้ขึ้นใจ 3 คำว่า “ไม่”

- ไม่เชื่อ**
 - ❌ ไม่เชื่อข้อความที่เร่งรัด
 - ❌ ไม่มีความน่าเชื่อถือ
 - ❌ ตรวจสอบกับหน่วยงานโดยตรง
- ไม่รับ**
 - ❌ อย่ากดลิงก์
 - ❌ อย่ารับไฟล์ข้อมูล
 - ❌ ดังสติ ตรวจสอบก่อน
- ไม่โอน**
 - ❌ ไม่โอนเงินแบบแลกหน้า
 - ❌ ไม่โอนเพื่อรับสิทธิ
 - ❌ ไม่โอนเพื่อยืนยันตัวตน

3 หากสงสัยว่าถูกหลอก

- ▶ **แจ้งสติ** หลีกเลี่ยงการธุรกรรม
- ▶ **เก็บหลักฐาน**
 - ☑️ รูปภาพ
 - ☑️ แฉก
 - ☑️ เลขบัญชี
 - ☑️ ลิงก์
- ▶ **แจ้งความออนไลน์** www.thaipoliceonline.go.th
- ▶ **ติดต่อธนาคารทันที** เพื่อยกเลิกบัญชี

4 สัญญาณเตือน

- ▶ รับโอนเงิน
- ▶ รับคดลิงก์
- ▶ ขอ OTP
- ▶ ขอข้อมูลส่วนตัว
- ▶ อ้างเป็นเจ้าหน้าที่รัฐ
- ▶ หลอกลวงลงทุน

อย่าหลงเชื่อ! มิจฉาชีพแฝงตัวมาในทุกรูปแบบ ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ

ไม่เชื่อ ไม่รับ ไม่โอน
ปลอดภัยกว่า 100%

ศูนย์ AOC 1441
สายด่วนออนไลน์
พร้อมช่วยเหลือตลอด 24 ชั่วโมง

ด้วยความห่วงใยจาก กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

เด็กก็เสี่ยง! “เปิดบัญชีม้า”

อย่าหลงเชื่อ “งานง่าย รายได้ดี” อาจเป็นกับดักของสแกมเมอร์

สแกมเมอร์มักหลอกล่อด้วยคำโฆษณา

- เปิดบัญชี รับ 2,000 บาท
- แค่สแกนหน้า ได้เงินทันที
- งานออนไลน์ ไม่ต้องลงทุน

Facebook
LINE
เกมออนไลน์
TikTok

สิ่งที่สแกมเมอร์ต้องการ

บัตรประชาชน → บัญชีธนาคาร → เบอร์โทรศัพท์ → Mobile Banking → สแกนใบหน้า (Face Scan)

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกลวง

มีบัญชีเพื่อเงินจากการหลอกลวง → เข้าบัญชีม้า → โอนต่อ/ถอนเงินออก → นำเงินไปใช้

วิธีป้องกัน

- ❌ ไม่เปิดบัญชีให้ใคร
- ❌ ไม่ให้ยืมบัญชีหรือซิม
- ❌ ไม่สแกนหน้าให้คนอื่น
- ❌ ไม่ส่ง OTP หรือรหัสผ่าน
- ❌ หากถูกชักชวนรับมัลแวร์ ไม่กดรับ หรือแจ้งตำรวจ

ผลที่ตามมา

- บัญชีถูกใช้รับเงินจากการหลอกลวง
- อาจถูกดำเนินคดีฐานเกี่ยวข้องกัน “บัญชีม้า” ผิดกฎหมาย
- บัญชีถูกอายัด ไม่สามารถใช้งานได้
- มีประวัติไม่ดี กระทบอนาคต เรียนต่อ ทำงาน สมัครงาน

ด้วยความห่วงใยจาก กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

พบเห็นการหลอกลวง แจ้งได้ที่ ☎ สายด่วนตำรวจไซเบอร์ 1441 | สายด่วน AOC 1441 | แจ้งความออนไลน์ www.thaipoliceonline.com

ระวัง! “รักออนไลน์” อาจเป็นกับดักหลอกล่อเงิน

ลูกหลานช่วยกันดูแลผู้สูงอายุ ก่อนตกเป็นเหยื่อ Romance Scam

มีงานง่าย รายได้ดี หลอกล่อด้วยความไว้วางใจ

สัญญาณเตือนที่ควรระวัง

- โปรไฟล์ดีเกินจริง**
 - รูปหล่อ สวย ดูดีเกินจริง
 - อาจใช้ภาพ AI หรือใช้รูปคนอื่น
- ทักษะหวาน รวดเร็ว**
 - เรียก “พี่รัก” “น้องรัก”
 - สร้างความสนิทใจไว้อย่างรวดเร็ว
- สุดท้ายขอเงิน**
 - ขอค่ารักษา / ค่าตัวเครื่องบิน
 - ค่าภาษี / อย่านอน
 - อ้างติดปัญหาไวรัสระบาด
- ไม่เคยเจอหน้าจริง**
 - อ้างติดงาน / อยู่ต่างประเทศ
 - วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

- 1 สร้างโปรไฟล์ปลอมให้น่าเชื่อถือ
- 2 ทักแชต คอยหวาน สร้างความผูกพัน
- 3 อ้างเหตุฉุกเฉิน ขอความช่วยเหลือ
- 4 หลอกให้โอนเงิน แล้วตัดการติดต่อ

จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน
หากไม่เคยพบตัวจริง อย่าโอนเงินเด็ดขาด!

ลูกหลานช่วยกันดูแลผู้สูงอายุ ก่อนตกเป็นเหยื่อ Romance Scam

ด้วยความห่วงใยจาก กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น กรมส่งเสริมการปกครองท้องถิ่น

หากสงสัยว่าเป็นมิจฉาชีพ แจ้งความออนไลน์ www.thaipoliceonline.go.th | สายด่วนตำรวจไซเบอร์ 1441